UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
08/814,409	03/11/1997	HIRONOBU KITAJIMA	826.1377/JPH	4623

21171 7590 05/21/2002

STAAS & HALSEY LLP
700 11TH STREET, NW
SUITE 500
WASHINGTON, DC 20001

EXAMINER
MEISLAHN, DOUGLAS J

ART UNIT	PAPER NUMBER
2132	24

DATE MAILED: 05/21/2002

Please find below and/or attached an Office communication concerning this application or proceeding.

UNITED STATES PATENT AND TRADEMARK OFFICE

COMMISSIONER FOR PATENTS
UNITED STATES PATENT AND TRADEMARK OFFICE
WASHINGTON, D.C. 20231
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Paper No. 24

Application Number: 08/814,409
Filing Date: March 11, 1997
Appellant(s): KITAJIMA ET AL.

Richard A. Gollhofer
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 13 February 2002.

(1) Real Party in Interest

A statement identifying the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

See section II of the brief.

(3) Status of Claims

The statement of the status of the claims contained in the brief is correct.

(4) Status of Amendments After Final

No amendment after final has been filed.

(5) Summary of Invention

The summary of invention contained in the brief is correct.

(6) Issues

The issues are whether claims 23-31 are properly rejected under 102(b) over Dabbish, whether claims 1-4, 6-8, 10-13, 15-17, and 19-22 are properly rejected under 103(a) over Dabbish in view of Knapp et al. and the Microsoft Press Computer Dictionary, and whether claims 9 and 18 are properly rejected under 103(a) over Dabbish in view of Knapp et al., the Microsoft Press Computer Dictionary, and Lynn et al. The appellant's statement of the issues in the brief is correct.

(7) Grouping of Claims

Appellant's brief includes a statement that claims 6 and 15 do not stand or fall together or with independent claims 1 and 10, that claims 7 and 16 stand and fall together but not with independent claims 1 and 10, and that claims 9 and 18 stand or

fall together but not with independent claims 1 and 10 and provides reasons as set forth in 37 CFR 1.192(c)(7) and (c)(8).

(8) Claims Appealed

The copy of the appealed claims contained in the Appendix to the brief is correct.

(9) Prior Art of Record

4972478	Dabbish	11-1990
5499192	Knapp et al.	03-1996
5345508	Lynn et al.	09-1994
The Microsoft Press Computer Dictionary, 3rd ed.		

(10) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 102

1. Claims 23-31 are rejected under 35 U.S.C. 102(b) as being clearly anticipated by Dabbish (4972478).

With respect to claim 23, elements 100 and 101 of figure 1 include PALs (Programmable Array Logic (Devices)) that are configured to encrypt or decrypt data. Thus the first clause of claim 23 is met.

Regarding the second clause, lines 56-58 of column 2, say that element 117, which is internal to the cryptographic circuit, receives cipher algorithm storage instructions from external programming equipment. This reception reads on "reading"

change data. The data is used to reprogram elements 100 and 101 and thus is change data.

With respect to the third clause, lines 59-61 of column 2 explain that the cipher algorithm storage instructions are used to reprogram the PALs. This usage reads on generating change data. This reception of the cipher algorithm, which accompanies use of the cipher algorithm storage instructions, imparts "automatically" to both clauses three and four of the claim. Lines 36-38 of column 1 anticipate the final clause of claim 23.

Claim 24 is a decrypting method identical to claim 23's encrypting method. Dabbish's PALs can perform both encryption and decryption operations and thereby meet the limitations of claim 24 in the same fashion as the limitations of claim 23. The sections cited with respect to either claim 23 or 24 meet claim 25. Claims 26-28 are apparatuses for claims 23-25. Claim 29 includes both encryption and decryption units. The claim does not mandate that these units are different. Encryption and decryption are not processes so much as end results – decrypting an unencrypted message will encrypt the message; thus the recitation of both encryption and decryption changing units is covered by Dabbish's single supervisory circuit.

With respect to claims 30 and 31, elements 100 and 101 read on the first clauses. As has been discussed previously, change commands originate with element 105, which is external to the cryptographic circuit. Element 103 is a network connecting unit and so reads on the second clauses. The supervisory circuit, element 102 of figure 1, reads on the third clauses of claims 30 and 31.

Claim Rejections - 35 USC § 103

2. Claims 1-4, 6, 8, 10-13, 15, 17, and 19-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dabbish (4972478) in view of Knapp et al. (5499192) and the Microsoft Press Computer Dictionary, 3rd ed.

The abstract in Dabbish discloses a " . . . logic cryptographic circuit that can be reprogrammed with various cipher algorithms." Reprogramming is a changing means. Changeable deciphering apparatus is disclosed in column 3, lines 44-46. In lines 51-67 of column one, Dabbish states that orders to change the encryption algorithm originate from sources external to the apparatus. He does not say that the change unit bases its decisions upon a mapping data object but does disclose an instruction program, stored in the supervisory circuit, handling the reprogramming of the crypto cores. Knapp et al.'s abstract and first four columns teach mapping data to programmable logic devices, saying that it can achieve greater convenience. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to use the common object-oriented programming to map instructions, as taught by Knapp et al., to the reprogrammable circuit of Dabbish. Knapp et al. do not say that a data object implements the mapping, but the computer dictionary teaches object-oriented programming as common.

There is no mention in this of an enclosure substantially surrounding the electrical components. Official notice is taken that it is old and well known to shield electrical components from the environment by surrounding them within an enclosure. One example of this is the case in which computer components reside. Therefore it

would have been obvious to a person of ordinary skill in the art at the time the invention was made to enclose the soft logic cryptographic circuit in Dabbish within protective material.

Claim 2's limitations are covered by Dabbish when the changes are considered in view of Knapp et al. Knapp et al. also teaches libraries and their associated elements in the paragraph spanning columns 3 and 4, thereby meeting claims 3, 4, and 6.

3. Claims 7 and 16 rejected under 35 U.S.C. 103(a) as being unpatentable over Dabbish, Knapp et al. and the computer dictionary as applied to claims 1 and 10 above.

Dabbish presents a system in which ciphering algorithms are written to a circuit, thus changing the algorithm that the circuit follows. Dabbish does not say that the algorithms are updated on a periodic basis. Official notice is taken that updating keys or other cryptographic devices is old and well known. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to allow for periodic updates of the circuit, making it particularly useful in time specific applications such as pay television systems.

4. Claims 9 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dabbish, Knapp et al. and the computer dictionary as applied to claims 1 and 10 above, and further in view of Lynn et al. (5345508).

Dabbish presents a system in which ciphering algorithms are written to a circuit, thus changing the algorithm that the circuit follows. The instructions to change the algorithm and the algorithm itself come from sources external to the circuit. Dabbish does not mention changing the circuits specifications based upon the communication

path, degree of communication path security, or the process speed required. Lynn et al. talk about changing encryption keys based upon processing time and security. They specifically describe how their invention can be used to balance these factors in the first paragraph of the brief summary, line 54 of column 2 through line 36 of column 3. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to allow for changes in the encryption circuits' specifications based upon the communication path, degree of communication path security, or process speed required as taught by Lynn et al. This would give flexibility to the system, letting it adapt to security and speed requirements.

(11) Response to Argument

Applicant posits that Dabbish '478 does not explain the process for reprogramming the crypto cores, elements 100 and 101. The first paragraph of the summary of the invention, lines 35-50 of column 1, refute this. In this section, Dabbish gives an outline for how the "cryptographic circuit can be programmed or reprogrammed" (lines 37-38). Beginning at line 48 of column 2, Dabbish gives a more detailed description of one way to program the cryptographic circuit. Dabbish et al. (4914697) is not part of the current rejection.

While the claims do contain the word "automatically" and applicant argues that this be given a particular meaning, the claims support only a broad interpretation because there is no specific event that triggers generating change data or changing a circuit structure. Thus any event, such as the external EPE program being read at the

input/output module 103, preceding these events reads on the "automatically" limitation of clauses 3 and 4 of claim 23 and similar language in other claims.

Applicant cites a portion of claims 30 and 31 as being distinct from the cited prior art and explains the discrepancy as the prior art showing "much more than a `command'". This is an admission that the cited prior art contains a command and renders the argument unpersuasive. As it is, any of the data sent from the EPE to the supervisory circuit or the crypto cores anticipates sending a command from the EPE. Changing circuit connections is anticipated by PALs, which are included in Dabbish's crypto cores.

Applicant goes on to question the combination of Dabbish and Knapp et al. Specifically, applicant does not feel that there is any suggestion to modify any specific part of Dabbish's apparatus according to the teachings of Knapp et al. The current rejection cites changing means in Dabbish. In lines 42-44 of column 1, Dabbish states that the crypto cores are reprogrammed specifically with the cipher algorithm storage instructions, which are stored in the supervisory circuit. The supervisory circuit is thus the changing means and would be the element that a person of ordinary skill in the art would be inclined to modify according to Knapp et al.

Knapp et al. teaches the content of claims 2-4 and 11-13, and the combination with Dabbish has already been discussed. Applicant states that nothing in the prior art has been cited with respect to "encrypted change data". In fact, this feature was first rendered obvious by official notice in the office action mailed 23 March 1999. Encrypting sensitive data is old and well-known, and a person using Dabbish's system

would be motivated to encrypt data sent from the EPE to the soft logic circuit. This encryption would deter eavesdroppers. Applicant lists some reasons that a person of ordinary skill in the art would not encrypt data transferred from the EPE to the supervisory circuit and crypto cores. While these reasons would discourage a person of ordinary skill in the art from encrypting data sent between, say, the EPE and the supervisory circuit, protecting the data from illicit viewing while in transit still would motivate a person of ordinary skill in the art to encrypt data sent from the EPE to the supervisory circuit and crypto cores.

Claim 15 stipulates that decrypted data is received. Any data that is not encrypted, that is, readable and intelligible, can be considered to be decrypted. Thus the data sent from the EPE to the supervisory circuit and crypto cores reads on claim 15. The structure of the claim makes the recitation of "decrypted" redundant because there is no reason to specify that data is decrypted when it was originally assumed to already be so.

With respect to claims 7 and 16, the rejections have already explained why periodic changes would be obvious. The invention and Dabbish are both clearly applicable to pay TV systems. Applicant's arguments regarding the rejection of claims 9 and 18 are the same as those against the rejection of claims 1 and 10 and are similarly unpersuasive.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Douglas J. Meislahn
Examiner
Art Unit 2132

DJM
May 15, 2002

Conferees
Gilberto Barron
Thomas Peeso

STAAS & HALSEY
700 ELEVENTH STREET N W
SUITE 500
WASHINGTON, DC 20001

GILBERTO BARRÓN
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100